WHAT IS CLAIMED IS:

1.   A person authentication system for executing person authentication by comparing a template which is person identification data acquired beforehand with sampling information input by a user, said system comprising an entity for executing person authentication, wherein said entity acquires a template from a person identification certificate storing temperature information including said template and generated by a third-party agency serving as a person identification certificate authority, and executes person authentication on the basis of the acquired template.

2.   A person authentication system according to Claim 1, wherein the person identification certificate issued by said person identification certificate authority includes a digital signature written by said person identification certificate authority.

3.   A person authentication system according to Claim 1, wherein said person identification certificate authority verifies the identification of a person requesting a person identification certificate to be issued, acquires a template serving as person identification data of said person requesting the person identification certificate to be

issued, and generates a person identification certificate storing template information including said template.

4. A person authentication system according to Claim 1, wherein, in the process of acquiring the person identification certificate from said person identification certificate authority, said entity performs mutual authentication between said entity and said person identification certificate authority, and said person identification certificate authority transmits the person identification certificate, provided that said mutual authentication is successfully completed.

5. A person authentication system according to Claim 1, wherein said person identification certificate authority stores said template in said person identification certificate after encrypting said template.

6. A person authentication system according to Claim 1, wherein said entity is any one of a service provider which makes a deal with a user identified by said person identification certificate, a user device accessed by a user identified by said person identification certificate, and said person identification certificate authority.

7. A person authentication system according to Claim 1, wherein, when transmitting said person identification certificate to said entity, said person identification certificate authority transmits a template which is stored in said person identification certificate, as an encrypted template which is decryptable only by said entity to which said person identification certificate is to be transmitted.

8. A person authentication system according to Claim 1, wherein said entity is a service provider which makes a deal with a user identified by said person identification certificate, and

wherein said service provider compares a template, which is acquirable from the person identification certificate acquired from said person identification certificate authority, with sampling information provided by the user and starts making a deal with the user, provided that said template and said sampling information match with each other.

9. A person authentication system according to Claim 1, wherein said entity is a user device serving as a data processing apparatus including data accessible by a user identified by said person identification certificate, and

wherein said user device compares a template, which is

acquirable from the person identification certificate acquired from said person identification certificate authority, with sampling information provided by the user, and said user device allows the user to start accessing said user device, provided that said template and said sampling information match with each other.

10. A person authentication system according to Claim 1, wherein said template is composed any one of biometric information of a person such as fingerprint information, retina pattern information, iris pattern information, voice print information, and handwriting information; non-biometric information such as a seal, a passport, a driver's license, and a card; any combination of two or more of said biometric information and said non-biometric information; and a combination of any of said information and a password.

11. A person authentication system according to Claim 1, wherein said entity and said person identification certificate authority have an encryption processing unit, respectively, and

wherein, when data is transmitted therebetween, mutual authentication is performed between said entity and said person identification certificate authority, a data-transmitting party generates a digital signature and adds it

to data to be transmitted, and a data-receiving party
verifies the digital signature.

12.   A person authentication system for executing
person authentication by comparing a template which is
person identification data acquired beforehand with sampling
information input by said person, said system comprising a
person identification certificate authority which acquires a
template from a person identification certificate storing
template information including said template, executes
person authentication on the basis of said acquired template,
and issues a verification certificate, provided that said
person authentication is successfully passed.

13.   A person authentication system according to Claim
12, wherein the verification certificate issued by said
person identification certificate authority includes a
digital signature written by said person identification
certificate authority.

14.   A person authentication system according to Claim
12, wherein said person identification certificate authority
verifies the identification of a person requesting a person
identification certificate to be issued, acquires a template
serving as person identification data of said person

requesting the person identification certificate to be
issued, and generates a person identification certificate
storing template information including said template.

15. A person authentication system according to Claim
12, wherein, in the process of acquiring the verification
certificate from said person identification certificate
authority, said entity performs mutual authentication
between said entity and said person identification
certificate authority, and said person identification
certificate authority transmits the verification certificate,
provided that said mutual authentication is successfully
completed.

16. A person authentication system according to Claim
12, wherein said entity acquiring the verification
certificate is one of a service provider which makes a deal
with a user identified by said person identification
certificate, and a user device accessed by a user identified
by said person identification certificate.

17. A person authentication system according to Claim
12, wherein said entity acquiring the verification
certificate is a service provider which makes a deal with an
user, and

wherein said service provider starts making a deal with the user, provided that the verification certificate is successfully acquired from said person identification certificate authority.

18. A person authentication system according to Claim 12, wherein said entity acquiring the verification certificate is a user device serving as a data processing apparatus including data accessible by an user, and

wherein said user device allows the user to start accessing said user device, provided that the verification certificate is successfully acquired from said person identification certificate authority.

19. A person authentication system according to Claim 12, wherein said entity acquiring the verification certificate verifies the signature of said verification certificate acquired from said person identification certificate authority and deletes said verification certificate after confirming that said verification of the signature indicates the validity of said verification certificate.

20. A person authentication system according to Claim 12, wherein said template is composed of any one of

biometric information of a person such as fingerprint information, retina pattern information, iris pattern information, voice print information, and handwriting information; non-biometric information such as a seal, a passport, a driver's license, and a card; any combination of two or more of said biometric information and said non-biometric information; and a combination of any of said information and a password.

21. A person authentication method for executing person authentication by comparing a template which is person identification data acquired beforehand with sampling information input by a user, wherein an entity for executing person authentication acquires a template from a person identification certificate storing template information including said template and generated by a third-party agency serving as a person identification certificate authority, and executes person authentication on the basis of the acquired template.

22. A person authentication method according to Claim 21, wherein said person identification certificate authority writes a digital signature on the person identification certificate issued by said person identification certificate authority.

23.   A person authentication method according to Claim 21, wherein said person identification certificate authority verifies the identification of a person requesting a person identification certificate to be issued, acquires a template serving as person identification data of said person requesting the person identification certificate to be issued, and generates a person identification certificate storing template information including said template.

24.   A person authentication method according to Claim 21, wherein, in the process of acquiring the person identification certificate from said person identification certificate authority, said entity performs mutual authentication between said entity and said person identification certificate authority, and said person identification certificate authority transmits the person identification certificate, provided that said mutual authentication is successfully completed.

25.   A person authentication method according to Claim 21, wherein said person identification certificate authority stores said template in said person identification certificate after encrypting said template.

26. A person authentication method according to Claim 21, wherein, when transmitting said person identification certificate to said entity, said person identification certificate authority transmits a template which is stored in said person identification certificate, as an encrypted template which is decryptable only by said entity to which said person identification certificate is to be transmitted.

27. A person authentication method according to Claim 21, wherein said entity is a service provider which makes a deal with a user identified by said person identification certificate, and

wherein said service provider compares a template, which is acquirable from a person identification certificate acquired from said person identification certificate authority, with sampling information provided by the user, and starts making a deal with the user, provided that said template and said sampling information match with each other.

28. A person authentication method according to Claim 21, wherein said entity is a user device serving as a data processing apparatus including data accessible by a user identified by said person identification certificate, and

wherein said user device compares a template, which is acquirable from a person identification certificate acquired

from said person identification certificate authority, with
sampling information provided by the user, and said user
device allows the user to start accessing said user device,
provided that said template and said sampling information
match with each other.

29.   A person authentication method for executing
person authentication by comparing a template which is a
person identification data acquired beforehand with sampling
information input by a user, wherein, at a person
identification certificate authority which acquires a
template from a person identification certificate storing
template information including said template and executes
person authentication on the basis of said acquired template,
a verification certificate is issued provided that said
person authentication is successfully passed.

30.   A person authentication method according to Claim
29, wherein said person identification certificate authority
writes a digital signature on the verification certificate
issued by said person identification certificate authority.

31.   A person authentication method according to Claim
29, wherein said person identification certificate authority
verifies the identification of a person requesting a person

identification certificate to be issued, acquires a template
serving as person identification data of said person
requesting the person identification certificate to be
issued, and generates a person identification certificate
storing template information including said template.

32. A person authentication method according to Claim
29, wherein, in the process of acquiring said verification
certificate from said person identification certificate
authority, said entity performs mutual authentication
between said entity and said person identification
certificate authority, and said person identification
certificate authority transmits the verification certificate,
provided that said mutual authentication is successfully
completed.

33. A person authentication method according to Claim
29, wherein said entity acquiring the verification
certificate is a service provider which makes a deal with an
user, and
    wherein said service provider starts making a deal with
the user, provided that the verification certificate is
successfully acquired from said person identification
certificate authority.

34. A person authentication method according to Claim
29, wherein said entity acquiring the verification
certificate is a user device serving as a data processing
apparatus including data accessible by an user, and

wherein said user device allows the user to start
accessing said user device, provided that the verification
certificate is successfully acquired from said person
identification certificate authority.

35. A person authentication method according to Claim
29, wherein said entity verifies the signature of said
verification certificate acquired from said person
identification certificate authority and deletes said
verification certificate after confirming that said
verification of the signature indicates the validity of said
verification certificate.

36. An information processing apparatus for executing
person authentication by comparing a template which is
person identification data acquired beforehand with sampling
information input by a user, wherein a template is acquired
from a person identification certificate generated by a
third-party agency serving as a person identification
certificate authority and storing template information
including said template, and person authentication is

executed on the basis of the acquired template.

37. An information processing apparatus according to
Claim 36, wherein the person identification certificate
issued by said person identification certificate authority
includes a digital signature written by said person
identification certificate authority, and said information
processing apparatus verifies the digital signature to check
whether or not data has been tampered with.

38. An information processing apparatus according to
Claim 36, wherein, in the process of acquiring a person
identification certificate from said person identification
certificate authority, said information processing apparatus
performs mutual authentication between said information
processing apparatus and said person identification
certificate authority, and said information processing
apparatus receives the person identification certificate,
provided that said mutual authentication is successfully
completed.

39. An information processing apparatus according to
Claim 36, wherein said information processing apparatus
compares a template, which is acquirable from the person
identification certificate acquired from said person

identification certificate authority, with sampling information provided by the user, and said information processing apparatus starts performing a process requested by the user, provided that said template and said sampling information match with each other.

40. A program providing medium for providing a computer program which executes, on a computer system, a person authentication process for executing person authentication by comparing a template which is person identification data acquired beforehand with sampling information input by a user, said computer program comprising the steps of:

acquiring a template from a person identification certificate generated by a third-party agency serving as a person identification certificate authority and storing template information including said template; and

executing person authentication on the basis of said acquired template.